MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2015/2016

TSN3251 and TSC2211 – COMPUTER SECURITY

(All Sections / Groups)

9 MARCH 2016
9:00 a.m. – 11:00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This paper consists of 7 pages (including cover page) with 5 Questions only.
2. Attempt **ALL FIVE** questions. The distribution of the marks for each question is given. This paper carries **100 marks**.
3. Please print all your answers in the Answer Booklet provided.

Question 1 (20 Marks)

a) State the "Principle of Adequate Protection" in computer security.

[1 mark]

b) Confidentiality, integrity and availability (CIA), is a model designed to guide policies for information security within an organization. In your own words, explain and give an example each on what is meant by the THREE (3) terms: **confidentiality**, **integrity** and **availability**.

[6 marks]

c) Differentiate between Cryptography, Cryptanalysis and Cryptology.

[3 marks]

d) Encryption algorithm may be breakable. Given enough time and data, a cryptanalyst can determine the plaintext message. State and briefly explain at least three types of cryptanalytic attacks.

[6 marks]

e) Briefly explain the terms used to classify threats: Interception, Interruption, Modification and Fabrication.

[4 marks]

Continued ...

Question 2 (20 Marks)

a) Encrypt the following sentence with key substitution cipher using the key "PASSED".

"this is such an easy exam"

In your answer, copy the following table to show how you did your encryption.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

[4 marks]

b) Decrypt the following message that was encrypted using the Playfair cipher with the key "anonymous". Ensure that you show each step you did to decrypt it clearly.

IAMEKNCZIZFUCV

[8 marks]

c) Given the following 2 by 2 matrix, $\begin{bmatrix} 4 & 5 \\ 3 & 1 \end{bmatrix}$, compute the inverse of the matrix in modulo 26 arithmetic.

$$\begin{bmatrix} 4 & 5 \\ 3 & 1 \end{bmatrix}^{-1}$$

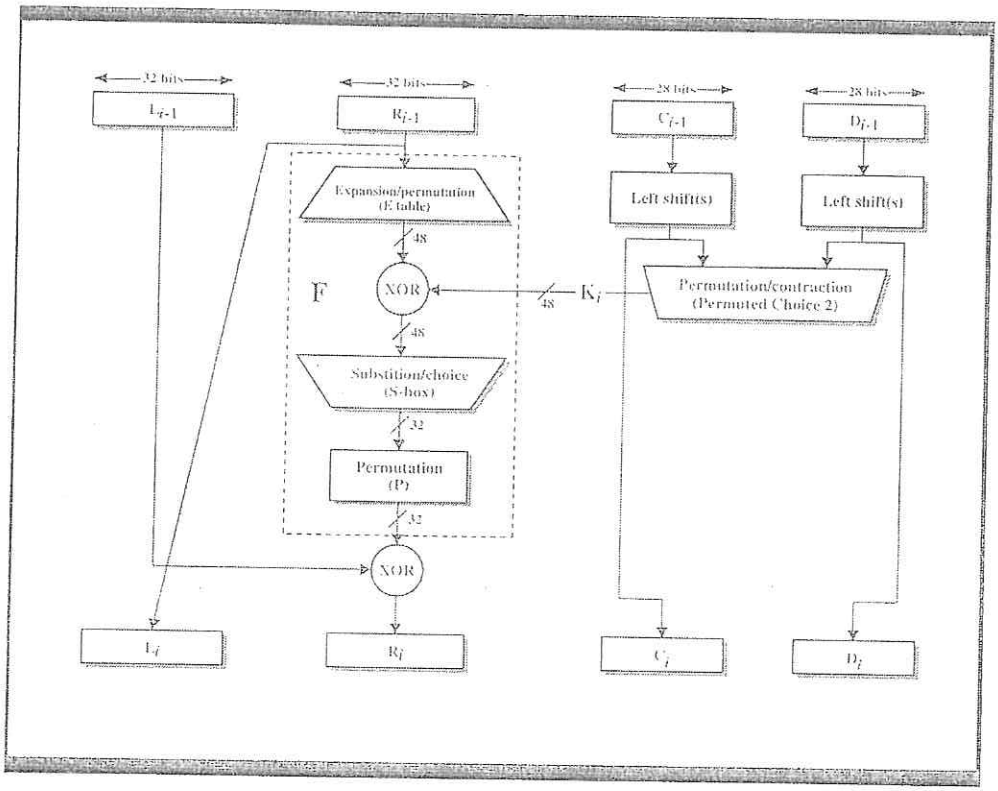
[8 marks]

Question 3 (20 Marks)

a) Explain why the Frequency Distribution method is not effective on ciphertext that has been encrypted using the transposition method. Also, state the goal of encryption by transposition as opposed to the substitution method.

[3 marks]

b) Modern ciphers combine both transposition and substitution cipher methods. One such popular cipher is the Data Encryption Standard (DEX). Consider the Single Round of the DES Algorithm as depicted in the figure below.



Given that L_3 is "1111 1111 0000 0001 0011 0110 0010 1111" and R_3 is "1101 1101 1101 0011 0101 1101 1010 1101". Use the *E Table* to compute the output after the Expansion/Permutation stage.

[5 marks]

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Expansion/Permutation (E)

Continued ...

c) Euler's Theorem is a generalization of the Fermat's theorem. It is stated as

$$a^{\phi(n)} \bmod n = 1, \text{ where } \gcd(a,n)=1$$

Show how you can solve $7^{503} \bmod 12$ using the Euler's Theorem (hint: you need some help from the square and multiply rule).

[8 marks]

d) RSA is the best known and most widely used algorithm for Public Key Cryptography. Describe the steps for RSA Key Generation.

[4 marks]

Question 4 (20 Marks)

a) Explain the steps for Birthday Attacks on Hash Functions.

[4 marks]

b) One of the drawbacks of using passwords as a form of authentication is "disclosure and revocation of access". Explain what is meant by this term.

[2 marks]

c) In a normal authentication process, the users key in their user identity followed by their passwords. List TWO (2) ways of enhancing this to prevent unauthorized authentication tries.

[2 marks]

d) State what is meant by the following FOUR (4) software threats.

- Virus
- Worms
- Trap Doors
- Rabbit

[4 marks]

e) Give an overview of Database SQL Injection attack and explain technically how it works. (You may use code snippet to explain if needed).

[4 marks]

Continued ...

f) Briefly describe 4 (out of the 7) issues that are addressed by a security plan.

[4 marks]

Question 5 (20 Marks)

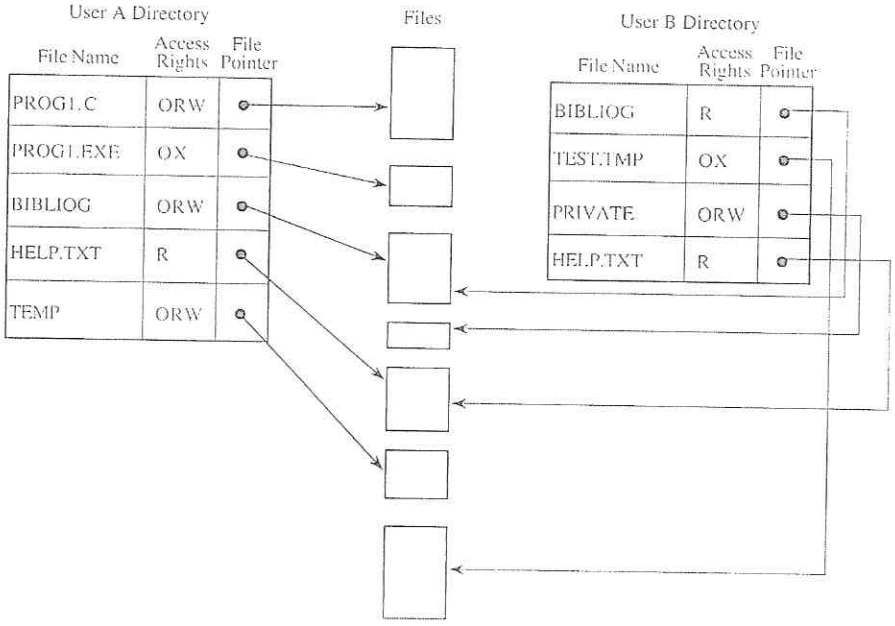
a) Briefly explain what is meant by "loose-lip" in assisting a password attack?

[2 marks]

b) In Operating System Access Security, what is the principle of least privilege? Why is it important?

[2 marks]

c) One of the simplest methods for file protection is to implement a directory listing of file permissions. This is a global list kept by the operating system and it is easy to implement, using one list per user in the system. This is illustrated below:-



State any THREE (3) drawbacks for such an implementation?

[3 marks]

Continued ...

d) In network security threats, explain the following terms.

i. Packet sniffing in wiretapping attacks

ii. Inductance in wiretapping attacks

iii. Phishing in Man-in-the-Middle attacks

[3 marks]

e) Differentiate between a Host Based Intrusion Detection System (IDS) and a Network Based IDS. Explain why a Host Based Intrusion Detection System (IDS) is more expensive to implement in a large organization as compared to Network Based IDS.

[2 marks]

f) There are many types of Denial of Service (DOS) attacks. One of them is called SYN-Flooding. Give a detailed explanation on how SYN-Flooding achieves a DOS.

[3 marks]

g) Provide the proper means of legal protection that can be applied for the following scenarios. Justify your answer on how the protection will be beneficial.

i) Alexis developed a new iOS application and she would like to publish it on Apple App Store but would like to protect her Intellectual Property prior to doing so

ii) Justin has thought of a new algorithm to determine the risk of a (car) driver which will be useful for insurance companies. He has coded the algorithm but is unable to test it as he does not have access to actual insurance data on drivers' profile and claims history. However, he would like to sell it to insurance companies but he also needs the data from the insurance companies. The insurance company needs assurance that his algorithm works and has asked him to present his solution to them, including how his algorithm works. Justin wants to protect his algorithm and setup a company to market the software but is unsure how. He has come to you to ask for advice. What would you advise him to do?

[2 + 3 marks]

END OF EXAM PAPER